TAYLOR MADE COMPUTER SOLUTIONS

ARE YOU PREPARING FOR GDPR?

On 25th May 2018 the EU's General Data Protection Regulation (GDPR) comes into effect across all the EU and EFTA member states, replacing the Data Protection Act in the UK (DPA), the Federal Data Protection Act in Germany (BDSG) and similar data privacy laws in all those states. It will be enforced by local data protection agencies and courts and provides for fines for defaulters of up to 4% of global turnover or, if higher, EUR 20m. It makes substantial changes to data protection rules in the UK.

GDPR tightens and extends the rules governing the processing of personal data by organisations but processing still means doing *anything* with it and personal data still means *any* information about an identifiable living individual. It could be just an email address.

New Rules

The key changes brought about by GDPR are:

- **Penalties** are increased. Now up to 4% of turnover or EUR 20m if higher.
- Both data controllers (the organisations deciding how the data is to be processed) and those that process it for them will have a new obligation to **document their data processing activities** so that they are able to demonstrate compliance with GDPR. That documentation will have to be comprehensive and regularly updated.
- Where two businesses share personal data and process it they need to **establish how their responsibilities under GDPR are shared**. That should be documented.
- **Data Processing Impact Assessments** should be carried out when a new type of processing is likely to result in a high risk for the rights and freedoms of the individual. For example if it includes medical or racial information or the risk of their identity theft. The assessment should contain a description of the processing operations to be undertaken by the processor, an assessment of the necessity and proportionality of the processing operations in relation to the purposes, an assessment of the risk to the rights and freedoms of data subjects, and the measures envisioned to address the identified risks including safeguards, security measures and mechanisms.
- Some organisations will need to appoint a **Data Protection Officer**. In reality every organisation will need to have someone who understands the complex legislation to keep them on the straight and narrow—that someone could be external.
- Data controllers must notify supervisory authorities (the Information Commissioner's Office in the UK) of a **personal data breach** within 72 hours of becoming aware of the breach, unless it is unlikely to result in a risk for the rights and freedoms of individuals.
- In some circumstances there is an **obligation to inform affected data subjects**.
- The requirement for **data subject consent** (when required at all) is much increased.
- There is an entirely new requirement to provide data subjects with **notices detailing how, why and when their data is being processed**.

- It now covers **data controllers based outside the EU** if the processing relates to the offering of goods or services to data subjects in the EU, or the monitoring of their behavior that takes place in the EU.

Data Processors

GDPR applies directly to both data controllers and processors. Processing carried out by a processor on behalf of a controller needs to be governed by a contract which needs to specify:

- that the processor should only act on instructions of the controller,
- that relevant staff would be under a duty of confidentiality,
- the necessary security and organisational measures that will be in place,
- that processing activities may only be sub-contracted with the prior consent of the controller,
- that the processor will assist the controller in making sure he complies with the necessary obligations in relation to data subjects and to data breach reporting,
- that the processor will return or erase any personal data on request by the controller at the end of the service contract,
- and make available to the controller and the relevant supervisory authority all necessary information regarding the processor's processing activities.

This would, for example, apply to a hosting contract. Many current hosting contracts are non-compliant or so complex that it can be difficult to establish whether they are compliant or not.

Consent

The requirement for consent to processing from data subjects, when required, is much strengthened. Consent now means the "freely given, specific, informed and unambiguous indication of the data subject's wishes" in a statement or by a "clear affirmative action". It is suggested that this spells the end of the "tick (or un-tick) box if you don't want…..". Furthermore the data subject will need to be informed of all the processing to be covered by his/her consent and the length of time that the processing is likely to continue. Records will need to be kept showing who has consented to what.

There are a number of alternatives to getting data subject consent to the processing which, because consent can be withdrawn, should be used whenever possible. E.g. the processing is *necessary* for the performance of a contract to which the data subject is a party or for pursuit of *legitimate* interests of the controller or a third party. These alternatives are generally not available where the processing is direct marketing. Interestingly however, recital 47 of the Regulations says that "processing…..for direct marketing purposes may be regarded as carried out for a legitimate interest." That appears to be a direct, though qualified (may be) contradiction to the general requirement of consent for direct marketing.

Notices

Notices detailing the proposed processing will need to be given to data subjects even if the data was obtained from a third party (E.g. if contained in a purchased contact list). Again there are some exceptions but these are of very limited use. The requirement to give these notices may impose a substantial administrative burden on many businesses.
For example, an email address is personal data. If you receive an email and do not delete it immediately you would appear to be processing the address (by holding it) and the same would apply to everyone that was ccd. Taken literally the Regulation will require you to send a notice to the sender and all who were ccd.

Joint Controllers

Businesses working together could be "joint controllers" of much of the data—as each is using it for its own purposes, not on behalf of the other. GDPR requires an "arrangement" between them setting out their respective roles and responsibilities. This suggests the need for amended co-operation or joint venture agreements or specific data processing agreements.

Interpretation

The GDPR is a creation of the EU and as such falls to be interpreted both "purposively" (what did Europe intend?) and proportionately (so as only to create obligations that are proportionate to the aims of the Regulation). Whilst that could be helpful in arguing that an apparent breach was not really a breach because that couldn't have been Europe's intention, it does make it very difficult to obtain certainty of interpretation. Where a business thinks it would be impossible to comply with some of the literal words of the Regulation and there is no specific exemption, it may be able to use purposive or proportionate to legitimise what otherwise would be non compliance.

Business to do list:

- Give a senior member of staff responsibility for implementing GDPR changes.
- Assess the personal data held by the business and how it is used.
- Identify any personal data that it is unnecessary to hold.
- Redesign information systems to avoid collecting or holding unnecessary personal data.
- Establish what processing requires consent and design systems for obtaining consent.
- Establish what processing requires notices to be sent to the data subjects.
- Update privacy notices/consent forms and their delivery mechanisms.
- Establish identity of any data processors/joint controllers and consider relevant contract terms.
- Produce a data processing statement setting out what, how, why etc.
- Don't forget that your customers may be asking you to demonstrate that you comply with GDPR.

Most SMEs will not have the internal expertise to re-design their processes and procedures to comply with GDPR and to interpret GDPR for that purpose. It is recommended that external expertise is engaged for this important task. With luck such a person will be able to assist in taking advantage of consent and notice exceptions to make compliance manageable.

Once a business has compliant processes and procedures in place, and documented its justifications for not doing anything that is too difficult by "purposive or proportionate" interpretation, then, unless its business is data processing, it will probably only require GDPR expertise on an occasional basis which could be covered by having an external "Data Protection Officer" to call on when necessary.

Penalties

Much has been made of the new penalties for non compliance and the headline figure of EUR 20m.

Although the Regulation does not say so, this does not really apply to you as an SME. It is there to make Google, Facebook, Amazon etc smart if they do not get it right. The general view is that no one is going to be at all interested in your compliance unless people start complaining about you or you are responsible for a major "data breach". Then your practices and procedures will be examined.

If you have made serious efforts to comply and can demonstrate that with your documentation, then you are likely to receive advice rather than punishment. If you have largely ignored the Regulation then you will be fined but the sum is likely to be proportionate to your size and resources.

What do you need to do now?

- Create a data “map” showing what personal data you process, where you get it from, what do you do with it, how long you keep it and with whom you share it.

- Analyse the map in the context of GDPR and make changes to your data processing where necessary for compliance.

- Create your “record” setting out what you do and how it is justified (lawful) under GDPR. This will include records of consents obtained from data subjects.

- Engage with your third party data processors and joint controllers (eg your data host) to ensure that compliant processing contracts are in place.

- Create any new documentation required, eg notices to be provided to data subjects.

- Set up systems to ensure continuing compliance and (probably) appoint a Data Protection Officer.